12-0

MPA
MOTION PICTURE ASSOCIATION
Audiovisual Entertainment
For Global Audiences

15503 Ventura Blvd.
Encino, CA 91436

TEL. (818) 995-6600
FAX: (818) 382-1797

VIA FACSIMILE

FAX SHEET CONFIDENTIALITY STATEMENT

DATE: December 28, 1999

TO: Nathan Knight

FROM: Mark D. Litvack
Los Angeles, Ca

SUBJECT: Linux CSS Development Analysis

Number of Pages: 30 (including cover)

PLEASE CALL TO CONFIRM RECEIPT. THANK YOU!

If there any problems in transmission, please call (818) 995-6600 ext. 374

MPA
MOTION PICTURE ASSOCIATION
Audiovisual Entertainment
For Global Audiences

15503 VENTURA BLVD.
ENCINO, CALIF. 91436

TEL: (818) 995-6600

ATTORNEY WORK PRODUCT
ATTORNEY CLIENT COMMUNICATION

DATE: December 23, 1999

DWG-19-99

TO:

Bob Lambert – Disney
Michele Kane – Disney
Lou Meisinger – Disney
Jane Sunderland – Fox
Mike Smarinsky – MGM
Laura Tunberg – MGM
Jared Jussim – Sony
Mitch Singer – Sony
Lucy Goldenhersh – Universal
W. Hanniball/J. Cates – Universal
Anat Levy – Viacom/Paramount
Steve Madoff – Viacom/Paramount
Chris Cookson – Warner
Marsha King – Warner

CC:

Jon Baumgarten – Proskauer Rose
Scott Cooper – Proskauer Rose
Bill Hart – Proskauer Rose
Tod Cohen – MPAA DC
Fritz Attaway – MPAA DC
Brad Hunt – MPAA
Ric Hirsch – MPAA
Simon Barsky - MPAA
Ken Jacobsen – MPAA

FROM: M. D. Litvack, Esq. MDL

SUBJECT: Linux CSS Development Analysis

NUMBER OF PAGES INCLUDING COVER: 29

Attached please the analysis submitted by Robert Schumann and CINEA. Because of time constraints, you are getting this before we discuss it with him. Should you have any questions, please contact me.

MPA
MOTION PICTURE ASSOCIATION
Audiovisual Entertainment
For Global Audiences

NATHAN G. KNIGHT, Jr.
Vice President
Regional Director, Anti-Piracy
Europe, Middle East & Africa

EUROPEAN OFFICE
Avenue de Tervueren, 270-272
B-1150 Brussels, Belgium
Tel (32-2) 778 27 11
Fax. (32-2) 778 27 50
E-mail nknight@mpaa.org

FAX MESSAGE

TO: Joachim Tielke
Managing Director
GVU

DATE: 19 January, 2000

STRICTLY CONFIDENTIAL

NOT FOR CIRCULATION

FAX#: (49-40) 611 792 40

CC: Jan Scharringhausen

FROM: Nathan Knight

RE: DVD Hack

NUMBER OF PAGES INCLUDING COVER: 29

Dear Jochen:

Please find attached a summary of the DVD Hack. I will call you later to discuss.

Kind regards.

Linux CSS Development Analysis

December 20, 1999

Robert Schumann
Cinea, LLC
12953 Oak Lawn Place
Herndon, VA 20171
(703) 346-0610
(703) 716-4644 (fax)

Table of Contents

Executive Summary

Cinea was engaged by the MPAA to review Linux DVD development forums to determine what, if any, role was played by group members in the breaking and release of the DVD CSS encryption system. Based on our detailed analysis, Cinea believes that some members of the Linux development community materially participated in the analysis and implementation of the CSS algorithms for the purpose of enabling DVD playback within the Linux environment. But there is no evidence that individuals in the Linux group provided critical breakthroughs. Our analysis indicates that the primary technical breakthroughs in Drive Authentication and Bulk content decryption were developed outside of the Linux development groups and were made available to the Linux groups. Our analysis indicates that one, Derek Fawcus, had contact with the various groups/individuals that provided the key technical breakthroughs and acted as a liaison between the external hacker community and the Linux development groups. Details of those contacts are not available in the material provided with the exception of Jon Johansson from the group MoRe, which released DeCSS in early October and Johan Addis who released the drive authentication, code in mid-July.

Analysis Overview

In late November 1999 Cinea was engaged by Mark Litvack of the MPAA to review several of the Linux DVD development forum lists and archives. The purpose of this analysis was to determine what, if any, role was played by members of these groups in the breaking and release of the DVD CSS encryption system. Additionally we reviewed these materials for the individual's motives in the breaking of CSS.

Cinea reviewed selections, provided by the MPAA in printed form, from the LinuxDVD and LividDEV discussion forums from June 1999 – November 1999. In addition Cinea did a cursory review of WEB addresses referenced throughout the archives. All of the following analysis and discussion is based solely on the materials provided to Cinea by the MPAA, and any visits to Web sites referenced in those materials.

The Linux development community is generally organized into small, loosely coupled groups, around common interests. These groups share a common belief in open and shared source code and a resultant freely licensed operating system. In almost all instances, the members of these groups work for free on personal time and are an eclectic collection of individuals. The Linux DVD groups reviewed here are no exception.

Based on our detailed analysis of the material, Cinea believes that some members of the Linux development community materially participated in the analysis and implementation of the CSS algorithms for the purpose of enabling DVD playback within the Linux environment. Our analysis indicates, however, that the primary technical breakthroughs in Drive Authentication and Bulk content decryption were developed outside of the Linux development groups and were made available to the Linux development groups.

Our analysis indicates that one, Derek Fawcus, had contact with the various groups/individuals that provided the key technical breakthroughs and acted as a liaison between the external hacker community and the Linux development groups. Details of those contacts are not available in the material provided with the exception of Jon Johansson from the group MoRe , which released DeCSS in early October, and Johan Addis who released the drive authentication code in mid July.

It is not clear from the materials available whether or not members of the Linux community initially published, or caused to be initially published, significant details of the CSS system. While there was much discussion of how the system worked and some members of the group were given information privately containing descriptions of the CSS algorithms there are no postings within the materials provided which are dated prior to other mentioned releases of the same information. Note that multiple members of the forum, including Derek Fawcus, volunteered to release the specifications but there is no indication whether this did or did not occur

It is important to note that there is no indication that the Linux development forums were focused on the development illegal copying systems. While many of the participants understood the potential of using open source systems as the basis for development of illegal copying capabilities, they would routinely go out of their way to publish and discuss the illegal nature of such acts. The intent of the community was clearly to develop legal and, if necessary, licensed playback environments which could then be legally distributed to enable DVD playback on Linux based computers.

Analysis Methodology

Cinea was provided with two large volumes of printed material by Mark Litvack of the MPAA. This material consisted primarily of copies of postings to two Linux development forums, LinuxDVD and LividDEV. These postings were dated from June through November of 1999 and appear to be a subset of the overall postings on these forums. The subset appears to have been selected based on relevance to the development of CSS enabled DVD playback.

Cinea read and analyzed all of the provided material. The purpose of this analysis was to build a timeline of related events and key participants in order to understand when and how the CSS system was broken and what, if any, of the Linux development communities participated in these efforts.

In addition to reviewing the provided materials Cinea also performed some cursory examination of relevant web sites referenced within the provided materials. In general these efforts added no additional value as almost all sites had been closed or the referenced material removed.

Prior to Cinea's involvement with this project the company, nor its employees involved (Robert Schumann and Rick Whittemore) had any detailed knowledge of the CSS architecture, and had and have never been privy to reviewing any official CSS related materials.

Timeline Review

This section describes the general time frame during which key developments were made. There are three identified windows: (a) from June 1999 through the breaking of CSS Authorization in mid July 1999; (b) then through first content decryption capabilities in mid September 1999; and (c) wide publication of keys and algorithms in October 1999.

Before entering the timeline it will be helpful to review that there are four distinct pieces of information needed to read CSS encrypted data on a PC. Until and unless all four pieces of information are available a full CSS implementation is not possible.

1. First the CSS disc authentication must take place. This authentication must occur once per disc inserted in the drive. Once the authentication is completed the drive is permitted to release encrypted sectors on the disc in the drive.
2. The overall data structures for key management and flow of keys and other information between the drive, data on the disc and the playback subsystem must be understood.
3. The actual CSS content encryption cipher (encryption algorithm) must be understood.
4. At least one Player key must be known in order to decrypt the content.

Now we can begin to discuss the timeline, where events will roughly follow the four pieces of information required.

a) Start – breaking of CSS Authorization
When the reviewed documents began in mid June the participants had already identified two phases to the overall CSS algorithm. The first phase was disc authentication, followed by the actual content decryption. Based on publicly distributed documents which describe the ATAPI disc drive interface, the general outline and commands needed to setup a DVD disc drive authentication are well known. The developers used this information to implement a DVD driver for the Linux environment. They were in the process of trying to understand the algorithms used to calculate the necessary keys and challenges necessary to complete the authentication.

Key players during this period were Paul Volcke who was coordinating the overall effort. Derek Fawcus who was actively trying to understand the algorithm using trial and error methods, and finally Andreas Bogk who said he was trying to acquire a CSS license while also observing the environment within the Windows domain.

This period ended on the 13th of July when a Johan Addis posted to the discussion group that he had Reverse Engineered the CSS disc authentication on a Windows machine and had code running since the beginning of 1999 which was able to setup sessions with a disc drive. Johan offered to release this code to the Linux community, and also said that he was working on Reverse Engineering the content decryption portion, so far without success. Johan never discussed why he embarked on these efforts or what his motivation was.

Johan's posting resulted in a flurry of activity on the board with significant discussions about the legality of posting his code and its use within a Linux playback environment. Johan was requested to not post the code on the LinuxDVD forum by its moderator due to potential legal issues. On the 14th of July, Johan released the code external to the reviewed Linux materials, it is not clear from the existing documentation where it was posted.

Following the release of the code by Johan, Derek Fawcus and others converted the code from assembler to 'C' code, debugged and enhanced it. This enhanced code was eventually widely distributed within the available development source trees. It is not

clear if any disc authorization code was ever incorporated within a "release" version of Linux.

b) First Decryption Capabilities

Following the posting of the disc authentication code the focus of the group shifted to the recovery of the disc keys and title keys necessary to decrypt the actual content on the disc. Once the disc is authenticated the drive is free to release encrypted content sectors to a read command. However, these encrypted sectors then also need to be decrypted using disc and title specific keys.

From mid July through the end of September the group discusses various potential structures of the CSS content encryption. From these discussions they begin to get an understanding of the structure in terms of how to identify encrypted sectors, that there are title and disc keys and that the cipher (encryption algorithm) is a block mode cipher with 40 bit keys. This data appears to have been determined through various analysis of the available data coming from the drive (after authorizing the transfers) as well as analysis of publicly available documents including Microsoft Windows API's and patent filings from Intel, Compaq, Cirrus and Oak. There are no indications that any of the direct participants on the list had any access to CSS specifications. In fact their missteps and misstatements would appear to indicate the opposite.

Derek Fawcus, however, continues to be a focal point for the feeding of information from the outside to the DVD development group. In late July (7/31) Derek reports that he was given a "major hint" on decoding a VOB file, but never identifies the source, or even if it is in reference to encryption or other characteristics of the VOB file. In Mid August (8/11) Derek indicates that he has been made aware of a potential CSS hack but has no firm information. There is no indication of whether this hack references the early rippers or a more substantial break of the CSS system. In late September Derek reports getting several purported CSS decryption systems, and on testing reports that they in fact seem to work. At this time Derek does not reveal any details of these hacks, only their existence. By mid October Derek reports that he now knows of five different individuals and/or groups which have crackers/algorithms for CSS and indicates that at least several of them were independently developed (Posting of Oct 11th on LividDEV). On October 27th Derek reports having posted the "beginnings" of a CSS algorithm description on his web site. This is his last substantive posting relative to this analysis.

Key discussion participants during this time are Derek Fawcus, Michael Holtz, Andreas Bogk, David MH, and Paul Volcko. Minor but interesting participants are Christian Wolff, and Martin Mueller. Several of these folks including Paul Volcko and Christian Wolff have legal access to the DVD specifications (but not the CSS specs). In general these individuals are very careful not to violate their DVD confidentiality. David MH never reveals his full identity and makes the first references to DVD rippers (powerrip and DvdRip) on the 18th of August. He later

returns, September 22 & 23rd, posting that he knows the group that wrote Speedripper (Drink or Die 'DoD') and that playback using these would not be legal.

In the middle of August the first 'Rippers' appear. These rippers, PowerRIP and DVDrip, are reviewed by various members of the group and the conclusion is that the rippers do not have access to the keys. The consensus was that they take advantage of loopholes in the Windows software implementations which allows the theft of decoded and/or decrypted content from the PC's memory.

During late September and early October there is much discussion of a full hack of CSS using Speedripper, first referenced by David MH on Sept 22nd. Speedripper was developed by a group called Drink-or-Die (Dod). The Speedripper is a partial solution, but appears to be missing some keys or key functionality, as it does not handle Warner Brothers Titles. Finally in early October the DeCSS program is discussed by Derek and finally released by Jon Johansson on the 6th of October. In later postings Jon confirms that he sent the source code for DeCSS to Derek as a release to the Linux community.

The hacker world is now able to fairly reliably remove CSS from DVD discs. The Linux community, however, still does not have a useful tool as both DeCSS and SpeedRip run only under Windows and no source is published.

c) Wide publication of Algorithm and Keys

Following the publishing of DeCSS there is widespread discussion on the forums about the legality of these systems. How they would be integrated, if at all, into a Linux environment, and continuing notices from many of the discussion members about the need to legally license the DVD stuff, the MPEG stuff and potentially the CSS stuff before any of this working code is useful to the Linux community. Relative to the legality of bypassing CSS without a license, there is extensive debate about whether use for playback within Linux, which is clearly the groups focus (including Derek Fawcus), constitutes a breach of various European and US Copyright laws (including Title 17 [ED ?? Correct name?]).

During early October there is an article published in the German computer magazine C't which discusses the CSS algorithm in a fair amount of detail. As a result of this article and the groups research and discussions, there is a fairly detailed knowledge of the exact nature of the key movement and handling. There is little knowledge (other than with Derek) of the actual Cipher (encryption algorithm), nor are any player keys known. Without keys or details of the Cipher the key passing algorithms are essentially useless, thus the focus of the group shifts to this last critical stage. The group realized that while they do not know the Cipher details the authors of DeCSS and SpeedRipper do and assume that the details of the Cipher will soon become known. Thus their primary focus is on how to get at more than one or two player keys.

During this period several anonymous posters release information, including a post on the 8th of October that getting at the player keys will not be a problem and that in 15 hours all 400 player keys can be extracted on a 400mhz Pentium PC. There is no indication of who posted this. On the 11th of October Derek Fawcus offers to bring together any interested parties in terms of arranging for the public release, or publishing, of the CSS algorithms and/or keys.

On the 26th of October, the source code to DeCSS appears to have been released , it is not evident where or by whom. Following this Aaron Holtzman writes his description of the algorithm since as he sees it "CSS code is now public" and thus he feels can discuss details openly.

This period culminates with the publishing by Frank Stevenson of his initial attacks against the CSS Ciphers. Frank is a new member to the list and describes his interest as Cryptographic. Frank later releases a scholarly paper which describes in complete detail the CSS cipher, a detailed analysis of its particular weaknesses, and how the weaknesses can be exploited to easily break the Cipher and gain access to the secrets. Frank appears to have done his analysis based on the source code to DeCSS.

Involvement of Key Individuals

Lunix Development Community

The following individuals were regular members of the Linux development community who's overriding efforts and interest were in the development of DVD playback capability within the Linux environment.

Andreas Bogk

Andreas Bogk is one of a handful of Germans on the site who contributors to the algorithm discussion. Andreas is interesting because he is pretty heavily involved in mid July, then essentially goes silent until early October when he rejoins the discussion of the algorithms. His insights are often keen. It is not clear what he was doing between Mid July and Early October.

Derek Fawcus

Derek Fawcus was a key member of the Linux DVD development environment with a particular emphasis on the enabling of playback of CSS protected movies under Linux. Derek participated actively in discussions about how CSS worked and how DVD drives and CSS could/should be incorporated within the Linux framework. In addition Derek did extensive code development and debugging of CSS related portions. In particular Derek took the drive authentication hack developed by Johan Addis and turned it into usable 'C' code within the Linux environment.

During this period several anonymous posters release information, including a post on the 8th of October that getting at the player keys will not be a problem and that in 15 hours all 400 player keys can be extracted on a 400mhz Pentium PC. There is no indication of who posted this. On the 11th of October Derek Fawcus offers to bring together any interested parties in terms of arranging for the public release, or publishing, of the CSS algorithms and/or keys.

On the 26th of October, the source code to DeCSS appears to have been released , it is not evident where or by whom. Following this Aaron Holtzman writes his description of the algorithm since as he sees it "CSS code is now public" and thus he feels can discuss details openly.

This period culminates with the publishing by Frank Stevenson of his initial attacks against the CSS Ciphers. Frank is a new member to the list and describes his interest as Cryptographic. Frank later releases a scholarly paper which describes in complete detail the CSS cipher, a detailed analysis of its particular weaknesses, and how the weaknesses can be exploited to easily break the Cipher and gain access to the secrets. Frank appears to have done his analysis based on the source code to DeCSS.

Involvement of Key Individuals

Lunix Development Community

The following individuals were regular members of the Linux development community who's overriding efforts and interest were in the development of DVD playback capability within the Linux environment.

Andreas Bogk

Andreas Bogk is one of a handful of Germans on the site who contributors to the algorithm discussion. Andreas is interesting because he is pretty heavily involved in mid July, then essentially goes silent until early October when he rejoins the discussion of the algorithms. His insights are often keen. It is not clear what he was doing between Mid July and Early October.

Derek Fawcus

Derek Fawcus was a key member of the Linux DVD development environment with a particular emphasis on the enabling of playback of CSS protected movies under Linux. Derek participated actively in discussions about how CSS worked and how DVD drives and CSS could/should be incorporated within the Linux framework. In addition Derek did extensive code development and debugging of CSS related portions. In particular Derek took the drive authentication hack developed by Johan Addis and turned it into usable 'C' code within the Linux environment.

Derek became a focal point of communications between the Linux development community and the apparently separate hacker community. It is clear that the hacker community was observing the efforts on the Linux board. In October they began to participate directly, through anonymous postings, prior to October they appear to have sent information to Derek.

In none of the postings is there any indication that Derek had any direct access to CSS specifications and in fact in several instances Derek makes statements which are clearly wrong. Similarly there is no indication that Derek actually completed any of the critical breakthroughs in terms of breaking the disc authentication or content decryption systems. Derek primarily used and enhanced other's work, while also discussing and reviewing the algorithms, as he understood them at any given point.

Finally, in the information provided, there is no clear evidence that Derek ever directly made public any of the information and source code made available to him by the hacker community. The only exception to this is a posting by Derek on the 27th of October where he states that he has posted the "beginning" of an algorithm description to his website. Note, however, that Derek did offer on several occasions, including the 11th of October, to facilitate the publishing of the algorithm.

Aaron Holtzman

Aaron Holtzman is primarily involved, until October, in the development of an AC-3 playback subsystem. In October he suddenly enters the CSS discussions with several posts on October 27th which indicate that he has studied the CSS algorithms in reasonable detail. Interestingly on the October 27th he posts an entry where he states his belief that the CSS code, algorithm and data are now public and thus he can freely discuss them. On October 28th an individual named 'aaron nonymous' posts some source for an unknown function (not described) other than the heading of the post which is "more code for reading/descrambling DVD". The name similarity between Aaron Holtzmann and 'Aaron nonymous' is striking given the context.

Michael Holtz

Michael Holtz is an interesting member of the community. Michael is not one of the members who is overly concerned with the legality of what is being accomplished. Michael is also very industrious in his finding out information about CSS. For example, in a series of posts on September 5th, he discussed the information he has gleaned from analyzing patent filings about CSS from Intel, Compaq, Cirrus and Oak. He also indicated familiarity with VideoCrypt and its inner workings. On September 30th he posts that he knows someone who Reverse Engineered a windows driver but wants to remain anonymous. Michael follows this with a post on October 1st wondering how anonymous folks can work together. Based on Michael's lack of information in early October it seems unlikely that Michael was one of the hackers, but he seems to be of that general mindset.

Nathan Laredo

Nathan Laredo is a new comer to the discussion group with his first posting on October 1st. He writes very assertively in his first posting about the nature of CSS encryption, describing the algorithm to be like RC4, and also says that the ability to read the encrypted files in WIN98 is a breach of the CSS licensing agreement. He never identifies how he knows that this is a breach. His last posting is on October 8th when he says that he heard a rumor that 40 player keys may soon be available. He never identifies the source of this rumor.

Paul Volcko

Paul Volcko was the overall organizer of the DVD on Linux development effort. Paul was working with a group of RIT (Rochester Institute of Technology) students on a legal DVD development effort in Linux called LSDVD (They had licensed the DVD specifications, bot NOT the CSS specifications). Paul would engage on speculation about how CSS worked but was continuously concerned that solutions needed to be developed that could be legally distributed. It should be noted that Paul and other members of the community became increasingly frustrated that they could not get any cooperation from the CSS licensing authority for their efforts.

There is no indication that Paul was involved directly in any of the CSS efforts other than open speculation and discussion of how the CSS algorithm worked.

External Contributors

The following posters were outsiders to the Linux development community who in general came into the discussion for brief periods of time, often providing critical source and information. These individuals generally provided no support to the Linux development efforts other than the release of information to the Linux community. They are likely members of the more general hacking community and in many cases posted anonymously.

Johan Addis

Johan is the clear source of the code which allowed the authentication of Discs and DVD drives. Johan was only active for a brief period in Mid July when he discussed that he had this code and eventually posted it, but not in this forum. It is not clear from the available material where the code was posted. The code created by Johan is then used by Derek and other in the community as the basis for the 'C' source included in the development source tree. During his posting, Johan mentions that he had the ability to authenticate to drives since early in 1999 and that he was also working on the content decryption but was not yet successful. There is no discussion of his motivation for these efforts.

Jon Johanson

Jon Johanson is the source of the posting and release of the DeCSS program. Jon in his various postings, starting in late September (23rd) and running through early November, is ambiguous about how the code was created. In most posts when talking

about DeCSS he says I. while in others he goes to lengths to describe "we or they" when talking about the creators of DeCSS. In his first post, done anonymously on the 23rd of September as "Digitech", he says that "Drink or Die" would never release source code but that a friend of his has similar code and he (Digitech) already has a copy. In any case, it is clear that Jon acted at least as a go between for the group MoRe and Derek Fawcus with both sides sending each other relevant source code.

David MH

David MH is the only unidentified semi-regular contributor to the postings. He posts only 3 relevant messages, but all three discuss rippers. The third posting on the 23rd of September identifies the source of "Speedripper" and David indicates the he understands it would not be legal.

Ghost XYZ

Ghost XYZ is an anonymous poster who placed a reference to an article on the 9th of October. There is no indication what this article contained, other than information on CSS. The URL referenced still contains four links, but these links are no longer valid.

Frank Stevenson

Frank Stevenson is a late entry into the discussions, posting his first entry on October 27th. Frank has a strong cryptographic background and ends up posting detailed scholarly discussions and papers on how CSS works and how to break the Ciphers used. In his paper[1], Frank states that all of his knowledge of CSS was gleaned from reviewing the posted source code for software claiming to be a descrambler. He further states that he has no access to any CSS information under NDA, nor has he read any official CSS documentation. There is no indication of why Frank focused on CSS other than an interest in things cryptographic.

Slamg ya

Slamg ya, an assumed pseudonym, posts a single entry on September 8th saying that he has been watching this forum the entire time and that people should look at several sites in germany which have papers on CSS. These papers are no longer available as the site dvdsoft.de has been shut down. The URL's were:
http://dvdsoft.de/filez/1394cp91.pdf and http://dvdsoft.de/filez/csspaper.pdf.

Open Questions/Issues

a) Why was a posting on Jon Johansonn on the 8th of October signed by "Jamie", and who is "Jamie?
b) Where did Johan Addis post his Disc authentication code?
c) Where was the DeCSS source code posted, and who posted it?

[1] Cryptanalysis of Contents Scrambling System. Frank A Stevenson (Frank@fluesteam.com). Unknown place of publication. 8th of November 1999 (Updated 13th November 1999)

Appendix A – Review Notes in date sorted order

Person	Date	Source	Comments
Paul Volcko	15-Jun	LinuxDVD	Folks at RIT are working on this project, but general stonewalling by manufacturers on support
Derek Fawcus	21-Jun	LinuxDVD	Knows of a site called wotsit.org, seems knowledgeable about how CSS works
Paul Volcko	22-Jun	LinuxDVD	Talks about CSS. Paul has access to the DVD specs (not CSS) and is checking into the licensing legalities
Aaron Holtzman	27-Jun	LinuxDVD	Wrote AC-3 decoder package in GPL.
Andreas Bogk	5-Jul	LinuxDVD	Says he is trying to acquire a CSS license
Paul Volcko	5-Jul	LinuxDVD	Lots of licensing talk. Talks about Andrew Veliath's work.
Andreas Bogk	13-Jul	LinuxDVD	Knows that the authentication is once per disc.
Derek Fawcus	13-Jul	LinuxDVD	More discussion of the data format while on the IDE/SCSI bus.
Derek Fawcus	13-Jul	LinuxDVD	Asks about the simplicity of the XOR
Johan Addis	13-Jul	LinuxDVD	Says that he has RE'd a PC player and has code which does the disc drive authentication. He is working on the frame decoding. Has had the authentication working since the beginning of the year.
Johan Addis	13-Jul	LinuxDVD	He RE'd the code using SoftIce and IDA
Michael Holtz	13-Jul	LinuxDVD	Encourages Johan to release the code
Paul Volcko	13-Jul	LinuxDVD	Asks some questions about CSS, thinks the encryption is DES. Starting to mentally build the system concept.
Derek Fawcus	14-Jul	LinuxDVD	Says he is willing to post the code for Johan. Also looked at code blocks and thinks bulk encryption is some block mode thing.
Johan Addis	14-Jul	LinuxDVD	He is holding the source code.
Ken Arondee	14-Jul	LinuxDVD	Shrink wrap license typically has a no RE clause?
Mathew Pavlovich	14-Jul	LinuxDVD	With full documentation for Matrox 6200 cards, with the CSS disc unlocking key he can start watching DVD's.

Person	Date	Source:	Comments
Mathew Pavlovich	14-Jul	LinuxDVD	Merge the code with Livid
Paul Volcko	14-Jul	LinuxDVD	Thinks Johan Addis should send the code to someone to post. Also says go for releasing it provided that it was not accomplished with access to the specs or an NDA.
Paul Volcko	14-Jul	LinuxDVD	If one is guiding others through the learning process RE is probably okay, but no direct use.
Paul Volcko	14-Jul	LinuxDVD	Apparently Johan released the code, Paul calls him brave.
Ralph Giles	14-Jul	LinuxDVD	Says post the code, elsewhere if need be to protect the Linux group.
Rolando Cedillo	14-Jul	LinuxDVD	To Johan, don't public post, but could he send a private copy?
Aaron Holtzman	15-Jul	LinuxDVD	Hasn't heard anything yet from Dolby.
Andreas Bogk	15-Jul	LinuxDVD	Bulk decryption code is still missing
Colin Davis	15-Jul	LinuxDVD	The release of the code should get the legal issues sorted out.
Didier Gautheron	15-Jul	LinuxDVD	Looking for an "easy to Chainsaw" emulator.
Mathew Pavlovich	15-Jul	LinuxDVD	Says that Johan's code and the code on slashdot are one and the same.
Michael Holtz	15-Jul	LinuxDVD	Thinks that only big-time pirates are a problem for the industry.
Paul Volcko	15-Jul	LinuxDVD	Something happened on slashdot? 'C' code update of the authorization code has appeared
Robert Homing	15-Jul	LinuxDVD	Dolby has lots of lawyers. He talks about having done DVD development
Andreas Bogk	16-Jul	LinuxDVD	Helping Michael debug the authentication code
Michael Holtz	16-Jul	LinuxDVD	Has a problem with the released code getting it to work.
Paul Volcko	17-Jul	LinuxDVD	See LinuxTV, Disc key blocks are longer (http://linuxtv.org).
Michael Holtz	18-Jul	LinuxDVD	Realizes that a title key is also needed.
Andreas Bogk	19-Jul	LinuxDVD	Title key is stored on a per sector bases [ED- I do not believe this is true]
Andreas Bogk	19-Jul	LinuxDVD	He does not have a CSS spec!
Christian Wolff	19-Jul	LinuxDVD	Working with LinuxTV, sounds like he knows lots of DVD details.
Derek Fawcus	19-Jul	LinuxDVD	Fixed the key access issues, and now gets consistent key block reads.

Person	Date	Source	Comments
Paul Volcko	19-Jul	LinuxDVD	Talks of the disc title structure
Paul Volcko	19-Jul	LinuxDVD	DVD .ifo files in http://linuxtv.org/dvd/ifs.html
Lodewijk Voge	20-Jul	LinuxDVD	Robocop, The Killer, Silence of the Lambs, all not CSS encrypted.
Ralph Giles	20-Jul	LinuxDVD	Highlander and Ghost in the Shell do not have CSS encryption.
Robert Horning	20-Jul	LividDev	Good discussion of legal options.
Derek Fawcus	21-Jul	LividDev	Has title key reading based on input from Martin Mueller.
Jens Axboe	21-Jul	LinuxDVD	Using the code, knows the CD-ROM commands very well.
Joachim Koenig	21-Jul	LividDev	VOB file player based on the NIST code? Must be only MPEG blocks.
Andreas Schildbach	25-Jul	LividDev	Why not look at the CSS code in a software decoder?
Martin Mueller	26-Jul	LividDev	Talks about the Pack headers and how to check for encryption.
Rob Lohman	26-Jul	LividDev	Creative Labs drive firmware upgrade.
Derek Fawcus	31-Jul	LividDev	Got a major hint from somebody on how to decode a VOB file.
Eric Smith	31-Jul	LividDev	Quick hack program to dump .ifo and .vob files that he had worked on.
Andreas Bogk	11-Aug	LinuxDVD	Has driver for MPEG-2, but financial risk is mentioned, plus some strange reference to Quantum bit encryption schemes.
Andreas Bogk	11-Aug	LinuxDVD	Has tested SCSI drives with CSS authentication code?
Derek Fawcus	11-Aug	LinuxDVD	Had info on potential Decryption hack, but no firm info available
Jens Axboe	11-Aug	LinuxDVD	Kernel 2.3.13 has IOCTRLS in it
Mathew Pavlovich	11-Aug	LinuxDVD	Knew status, said 2.4 has IOCTRLS for drives in it
Paul Volcko	11-Aug	LinuxDVD	Asking for status of the development project
Marshall Goldberg	16-Aug	LividDev	From Sigma designs, looks to muster support for a Linux development effort with Sigma.
Paul Volcko	16-Aug	LividDev	Mentions that DVD drive access is now enabled thanks to work done by Andrew Veliath @ RPI.
Derek Fawcus	17-Aug	LividDev	Only the Authorization work is done, decryption still needs to be completed.

Person	Date	Source	Comments
David MH	18-Aug	LividDev	Says he knows of 2 ripers, PowerRipper and DVD rip, but claims he has no DVD drive. In a "dream mode scenario" someone would find specs, but he does not already have them.
Michael Holtz	18-Aug	LividDev	Knows, or claims to know, how powerrip and DVDRip work, by taking video out of the display windows.
Nicholas Strugnell	18-Aug	LividDev	Says that rippers are perfectly legal, claims knowledge that using and developing are legal. Says in CSS the algorithm is secret.
Nicholas Strugnell	18-Aug	LividDev	Is working on getting the Matrox card to work.
Paul Volcko	22-Aug	LividDev	Had clearly analyzed the available rippers and knows that DVDRip does ripping before decode. He surmises how they function. Says that any Linux software based DVD player would also be broken the same way.
Joachim Koenig	23-Aug	LividDev	Did the MPEG-2 player code optimized for MXX
Martin A. Sato	24-Aug	LividDev	Agrees that segmentation of the Sigma DVD library would be good.
Paul Volcko	24-Aug	LividDev	He is part of the LSDVD project. They have access to the full DVD specifications and are writing a legal player. But no CSS specs!
Ralph Giles	26-Aug	LividDev	Talks about a statement by Bruce Scheier who says that "crypoanalysts and hackers don't do reverse engineering". He (Paul) further seems to imply that DCD Cipher and Firewire cipher have been broken in contests. Www.counterpane.com/crypto-gram-9812.html#contests
Eric Smith	3-Sep	LividDev	Provided details on the subpicture structure, appears to be very detailed.
Hetz Ben Hamo	4-Sep	LividDev	Says he saw article that RE is legal in Australia
Eric Smith	5-Sep	LividDev	Provides link to the Digital Millenium Copyright Act (http://uscode.house.gov/title_17.htm)
Ian Wade	5-Sep	LividDev	Bursts Hetz's bubble by saying that the law appears targeted at Y2K issues.
Michael Holtz	5-Sep	LividDev	Talks of patents and keys. Knows the structure of VideoCrypt.
Michael Holtz	5-Sep	LividDev	Posts results of a patent search. Several interesting nuggets appear by Intel, Cirrus, Compaq and Oak.
Michael Holtz	5-Sep	LividDev	Followed the links in Cpmaq patent to http://reality.sgi.com/memec/dvd.html

Person	Date	Source	Comments
slamg ya	8-Sep	LividDev	Says he has been watching the whole time and says to look at several sites in Germany. Http://dvdsoft.de/filez/1394cp91.pdf and http://dvdsoft.de/filez/csspaper.pdf
Ralph Metzler	11-Sep	LividDev	Is doing DVB and DVD stuff has some video playing from unencrypted VOBS. Uses a hardware card and is looking for CP to happen on that card.
David MH	22-Sep	LividDev	Says to get Speedripper from DVDsoft.de. He says that he has read documentation (for speedripper?).
Eliot Landrum	22-Sep	LividDev	Replies to a post from DMH that says that CSS has been cracked, Eliot asks where the source is.
David MH	23-Sep	LividDev	Says that someone (thing?) called "Drink or Die" (DOD) was the one releasing speedripper, also indicated he knows that playback would not be legal.
Jon Johanson posting as digitech	23-Sep	LividDev	Says that Drink or Die would never release code, but a friend of his has similar code and he already has a copy.
Derek Fawcus	30-Sep	LinuxDVD	Points to or knows of CSS code
Michael Holtz	30-Sep	LividDev	Knows someone who RE'd windows driver for the Creative DXR2 and he is trying to write a windows version, but wants to remain anonymous.
Bryan Olson	1-Oct	LividDev	Talks about CSS keys and guesses at the number of player keys.
Derek Fawcus	1-Oct	LividDev	Says he has received several claimed CSS decryption algorithms written in 'C' and 'asm' but has not had a chance to test.
Martin Mueller	1-Oct	LividDev	German computer magazine C'T has text about CSS (www.heise.de/ct)
Michael Holtz	1-Oct	LividDev	Wondering how anonymous folks can work together
Nathan Laredo	1-Oct	LividDev	Writes very assertively about the nature of CSS encryption, including that the algorithm is like RC4. Also says that the ability to read the encrypted files in WIN98 is a breach of the CSS license (How does he know?).
Nathan Laredo	1-Oct	LividDev	Adds more detail in a following post to Paul.
Paul Volcko	1-Oct	LividDev	Recognizes the nature of RE is shady and suggests that people who want to work in that space should use anonymous remailers and encryption to protect and sign their stuff.

Person	Date	Source	Comments
Derek Fawcus	2-Oct	LividDev	The CSS decryption algorithms work, describes the algorithm and his desire to hold back the key.
Derek Fawcus	2-Oct	LividDev	His suppliers have confirmed that his key is the same as the key for dodsrip
Martin Mueller	2-Oct	LividDev	C't magazine says that dodsrip only contains a fraction of a player key? Www.heise.de/newsticker/data/ghi-28.09.99-000
Aaron Holtzman	4-Oct	LividDev	CSS algorithm already has been cryptoanalyzed and broken just not published Remark by Bruce Schneier about this in past.
Andreas Bogk	4-Oct	LividDev	He is still paying attention, and participating in the algorithm discussion.
Christian Wolff	4-Oct	LividDev	Writes about C't article which says that DVD region code would be enforced by the drive.
Derek Fawcus	4-Oct	LividDev	The group has the overall algorithm defined now, and are looking for ways to extract player keys, potentially using brute force analysis of the cyphertext.
Michael Holtz	4-Oct	LividDev	Looking for algorithm from Derek.
Paul Volcko	4-Oct	LividDev	Why don't they just make a piece of cracker code so that implementations would not need to ship with a key, thus a copy on a machine could calculate a key once it is trying to be used. This way a on-enabled version (IE no key) is shipped.
Thomas "Dent" Mirlacher	4-Oct	LividDev	Put the latest version of the .ifo file parser out as source. Big disclaimer that he had no access to specs, nor did any individuals provide him info directly.
Dimitry Gromov	5-Oct	LividDev	Writes about Cnet article from 8/22/97 which says that CSS is cracked. Includes discussion of bootlegs in China and Russia. Theorizes that dodsrip is based on a ripoff of bootleggers code.
Derek Fawcus	6-Oct	LividDev	He has the source to DeCSS and complains that they used his authentication code without giving him credit.
Derek Fawcus	6-Oct	LividDev	Says he got the source by "A little birdy told me".
Jon Johanson	6-Oct	LividDev	Posts the DeCSS code!
Jon Johanson	7-Oct	LividDev	Writes that he sent source to his connection in Linux community (later identified as Derek).
Ted Milker	7-Oct	LividDev	Points to DeCSS source code at: http://mmadb.no/hwlpus/___MMSystem_275___/Decss.zip

Person	Date	Source	Comments
Tod Milker	7-Oct	LividDev	Writes that the source WAS there as he has a copy.
Anonymous	8-Oct	LividDev	Says player keys won't be a problem. 15 Hours for all 400 keys ona dual pentium.30 additional hours if you do not know the title key yet. Players do and can have more than 1 key?
Bryan Olson	8-Oct	LividDev	Says that binary is almost as bad as source since the consortium would be able to figure out the key found from the binary. Also asks for reference for the $1,000,000 damage claim.
Bryan Olson	8-Oct	LividDev	He has also seen the license agreement as he says that it is only related to a material breach.
David Barth	8-Oct	LividDev	The usal Suspects is Unencrypted
Jon Johanson	8-Oct	LividDev	Says that he got code directly from Derek with a license to use.
Jon Johanson	8-Oct	LividDev	They (meaning the creators of DeCSS) gave source to Derek to do with as he see's fit.
Jon Johanson	8-Oct	LividDev	Posted that there is no source on the page pointed to by Ted. Interestingly this page was signed by a "Jamie"
Michael Holtz	8-Oct	LividDev	Totally pissed off at Jon Johanson. Says that he wants to RE it himself.
Nathan Laredo	8-Oct	LividDev	Don't release the source as it will get a commercial company in trouble. Post an analysis of the algorithm to sci.crypt and let the them hack it. He says a "little Birdie" tells him that a linux binary of Dodsrip will be released to Linux soon.
Nathan Laredo	8-Oct	LividDev	Writes that the CSS license agreement is available from MEI.
Nathan Laredo	8-Oct	LividDev	Says that he heard a rumor that 40 players keys may soon be available.
GhostZYX	9-Oct	LividDev	Says to checkout the paper at http://members.xoom.com/sihat2 (ED: 4 links are still there, but what they point to has been removed).
Christian Wolff	11-Oct	LividDev	Has specs and signed NDA for DVD spec related to IFO file parsing.
Derek Fawcus	11-Oct	LividDev	Returns from being away to lots of info. He has new sources for DeCSS which add to the overall algorithm. Now knows a total of 5 people who have algorithm. At least two have brute forced the algorithm. Offers to bring people together.
Didier Gautheron	11-Oct	LividDev	Has pieces of the IFO file parsing, looking for somewhere to upload it to.
Joachim Koenig	20-Oct	LividDev	Working on a NIST version which could play DVD's directly

Person	Date	Source	Comments
Aaron Holtzman	26-Oct	LividDev	Says CSS code now public and he discusses the algorithm and data as he sees it.
Adam Pennington	26-Oct	LividDev	Has read the last several posts and has the source, but not in Linux ported form. Looking for info.
Aaron Holtzman	27-Oct	LividDev	Replies to a query with details of the salting of the decryption algorithm.
Aaron Holtzman	27-Oct	LividDev	Comments on code from Phil Burr about the hash function, that it is non reversible as such.
Aaron Holtzman	27-Oct	LividDev	After further study he stands corrected and the hash is reversible.
Derek Fawcus	27-Oct	LividDev	Posted the beginning of his description of the algorithm at: www.eyrie.demon.co.uk/derek/dvd/css/cssinfo.html. (ED: This file is now gone, as are all of Derek's files).
Frank Stevenson	27-Oct	LividDev	Posts the crack code to get at the keys. Also is a new member & just posted
Phil Burr	27-Oct	LividDev	Posts comments on brute forcing a private player key.
aaron nonymous	28-Oct	LividDev	Posts source code for ???. Title is more code for reading/descrambling DVD.
aaron nonymous	29-Oct	LividDev	Posts the title key for matrix
MRS	29-Oct	LividDev	Looking for someone to send him a decrypted disk key from 5-20 DVDs along with matching title keys (encrypted and decrypted), wants to try something.
Frank Stevenson	30-Oct	LividDev	Posts an attack for the disc key from the hash at the beginning of the datablock.
Yuging Deng	30-Oct	LividDev	Posts code for CSS-Auth which has a whole table of player key structures.
Jon Johanson	2-Nov	LividDev	Jon is also the name Digitech (does posting with both names)

Appendix B -- Review Notes in posting name sorted order

Person	Date	Source	Comments
Aaron Holtzman	27-Jun	LinuxDVD	Wrote AC-3 decoder package in GPL.
Aaron Holtzman	15-Jul	LinuxDVD	Hasn't heard anything yet from Dolby.
Aaron Holtzman	4-Oct	LividDev	CSS algorithm already has been cryptoanalyzed and broken just not published Remark by Bruce Schneier about this in past.
Aaron Holtzman	26-Oct	LividDev	Says CSS code now public and he discusses the algorithm and data as he sees it.
Aaron Holtzman	27-Oct	LividDev	Replies to a query with details of the salting of the decryption algorithm.
Aaron Holtzman	27-Oct	LividDev	Comments on code from Phil Burr about the hash function, that it is non reversible as such.
Aaron Holtzman	27-Oct	LividDev	After further study he stands corrected and the hash is reversible.
aaron nonymous	28-Oct	LividDev	Posts source code for ???. Title is more code for reading/descrambling DVD.
aaron nonymous	29-Oct	LividDev	Posts the title key for matrix
Adam Pennington	26-Oct	LividDev	Has read the last several posts and has the source, but not in Linux ported form Looking for info.
Andreas Bogk	5-Jul	LinuxDVD	Says he is trying to acquire a CSS license
Andreas Bogk	13-Jul	LinuxDVD	Knows that the authentication is once per disc.
Andreas Bogk	15-Jul	LinuxDVD	Bulk decryption code is still missing
Andreas Bogk	16-Jul	LinuxDVD	Helping Michael debug the authentication code
Andreas Bogk	19-Jul	LinuxDVD	Title key is stored on a per sector bases [ED- I do not believe this is true]
Andreas Bogk	19-Jul	LinuxDVD	He does not have a CSS spec!
Andreas Bogk	11-Aug	LinuxDVD	Has driver for MPEG-2, but financial risk is mentioned, plus some strange reference to Quantum bit encryption schemes.
Andreas Bogk	11-Aug	LinuxDVD	Has tested SCSI drives with CSS authentication code?
Andreas Bogk	4-Oct	LividDev	He is still paying attention, and participating in the algorithm discussion.
Andreas	25-Jul	LividDev	Why not look at the CSS code in a software decoder?

Person	Date	Source	Comments
Schildbach			
Anonymous	8-Oct	LividDev	Says player keys won't be a problem. 15 Hours for all 400 keys ona dual pentium.30 additional hours if you do not know the title key yet. Players do and can have more than 1 key?
Bryan Olson	1-Oct	LividDev	Talks about CSS keys and guesses at the number of player keys.
Bryan Olson	8-Oct	LividDev	Says that binary is almost as bad as source since the consortium would be able to figure out the key found from the binary. Also asks for reference for the $1,000,000 damage claim.
Bryan Olson	8-Oct	LividDev	He has also seen the license agreement as he says that it is only related to a material breach.
Christian Wolff	19-Jul	LinuxDVD	Working with LinuxTV, sounds like he knows lots of DVD details.
Christian Wolff	4-Oct	LividDev	Writes about C't article which says that DVD region code would be enforced by the drive.
Christian Wolff	11-Oct	LividDev	Has specs and signed NDA for DVD spec related to IFO file parsing.
Colin Davis	15-Jul	LinuxDVD	The release of the code should get the legal issues sorted out.
David Barth	8-Oct	LividDev	The usal Suspects is Unencrypted
David MH	18-Aug	LividDev	Says he knows of 2 ripers, PowerRipper and DVD rip, but claims he has no DVD drive. In a "dream mode scenario" someone would find specs, but he does not already have them.
David MH	22-Sep	LividDev	Says to get Speedripper from DVDsoft.de. He says that he has read documentation (for speedripper?).
David MH	23-Sep	LividDev	Says that someone (thing?) called "Drink or Die" (DOD) was the one releasing speedripper, also indicated he knows that playback would not be legal.
Derek Fawcus	21-Jun	LinuxDVD	Knows of a site called wotsit.org, seems knowledgeable about how CSS works.
Derek Fawcus	13-Jul	LinuxDVD	More discussion of the data format while on the IDE/SCSI bus.
Derek Fawcus	13-Jul	LinuxDVD	Asks about the simplicity of the XOR
Derek Fawcus	14-Jul	LinuxDVD	Says he is willing to post the code for Johan. Also looked at code blocks and thinks bulk encryption is some block mode thing
Derek Fawcus	19-Jul	LinuxDVD	Fixed the key access issues, and now gets consistent key block reads.

Person	Date	Source	Comments
Derek Fawcus	21-Jul	LividDev	Has title key reading based on input from Martin Mueller.
Derek Fawcus	31-Jul	LividDev	Got a major hint from somebody on how to decode a VOB file.
Derek Fawcus	11-Aug	LinuxDVD	Had info on potential Decryption hack, but no firm info available
Derek Fawcus	17-Aug	LividDev	Only the Authorization work is done, decryption still needs to be completed.
Derek Fawcus	30-Sep	LinuxDVD	Points to or knows of CSS code
Derek Fawcus	1-Oct	LividDev	Says he has received several claimed CSS decryption algorithms written in 'C' and 'asm' but has not had a chance to test.
Derek Fawcus	2-Oct	LividDev	The CSS decryption algorithms work, describes the algorithm and his desire to hold back the key.
Derek Fawcus	2-Oct	LividDev	His suppliers have confirmed that his key is the same as the key for dodsrip.
Derek Fawcus	4-Oct	LividDev	The group has the overall algorithm defined now, and are looking for ways to extract player keys, potentially using brute force analysis of the cyphertext.
Derek Fawcus	6-Oct	LividDev	He has the source to DeCSS and complains that they used his authentication code without giving him credit.
Derek Fawcus	6-Oct	LividDev	Says he got the source by "A little birdy told me".
Derek Fawcus	11-Oct	LividDev	Returns from being away to lots of info. He has new sources for DeCSS which add to the overall algorithm. Now knows a total of 5 people who have algorithm. At least two have brute forced the algorithm. Offers to bring people together.
Derek Fawcus	27-Oct	LividDev	Posted the beginning of his description of the algorithm at: www.eyrie.demon.co.uk/derek/dvd/css/cssinfo.html. (ED: This file is now gone, as are all of Derek's files).
Didier Gautheron	15-Jul	LinuxDVD	Looking for an "easy to Chainsaw" emulator.
Didier Gautheron	11-Oct	LividDev	Has pieces of the IFO file parsing, looking for somewhere to upload it to.
Dimitry Gromov	5-Oct	LividDev	Writes about Cnet article from 8/22/97 which says that CSS is cracked. Includes discussion of bootlegs in China and Russia. Theorizes that dodsrip is based on a ripoff of bootloggers code.
Eliot Landrum	22-Sep	LividDev	Replies to a post from DMH that says that CSS has been cracked, Eliot asks where the source is.
Eric Smith	31-Jul	LividDev	Quick hack program to dump .ifo and .vob files that he had worked on.

Person	Date	Source	Comments
Eric Smith	3-Sep	LividDev	Provided details on the subpicture structure, appears to be very detailed.
Eric Smith	5-Sep	LividDev	Provides link to the Digital Millenium Copyright Act (http://uscode.house.gov/title_17.htm)
Frank Stevenson	27-Oct	LividDev	Posts the crack code to get at the keys. Also is a new member & just posted.
Frank Stevenson	30-Oct	LividDev	Posts an attack for the disc key from the hash at the beginning of the datablock.
GhostZYX	9-Oct	LividDev	Says to checkout the paper at http://members.xoom.com/sihat2 (ED: 4 links are still there, but what they point to has been removed).
Hetz Ben Hamo	4-Sep	LividDev	Says he saw article that RE is legal in Australia
Ian Wade	5-Sep	LividDev	Bursts Hetz's bubble by saying that the law appears targeted at Y2K issues.
Jens Axboe	21-Jul	LinuxDVD	Using the code, knows the CD-ROM commands very well.
Jens Axboe	11-Aug	LinuxDVD	Kernel 2.3.13 has IOCTRLS in it
Joachim Koenig	21-Jul	LividDev	VOB file player based on the NIST code? Must be only MPEG blocks.
Joachim Koenig	23-Aug	LividDev	Did the MPEG-2 player code optimized for MXX
Joachim Koenig	20-Oct	LividDev	Working on a NIST version which could play DVD's directly
Johan Addis	13-Jul	LinuxDVD	Says that he has RE'd a PC player and has code which does the disc drive authentication. He is working on the frame decoding. Has had the authentication working since the beginning of the year.
Johan Addis	13-Jul	LinuxDVD	He RE'd the code using SoftIce and IDA
Johan Addis	14-Jul	LinuxDVD	He is holding the source code.
Jon Johanson	6-Oct	LividDev	Posts the DeCSS code!
Jon Johanson	7-Oct	LividDev	Writes that he sent source to his connection in Linux community (later identified as Derek).
Jon Johanson	8-Oct	LividDev	Says that he got code directly from Derek with a license to use.
Jon Johanson	8-Oct	LividDev	They (meaning the creators of DeCSS) gave source to Derek to do with as he see's fit.
Jon Johanson	8-Oct	LividDev	Posted that there is no source on the page pointed to by Ted. Interestingly this page was signed by a "Jamie"
Jon Johanson	2-Nov	LividDev	Jon is also the name Digitech (does posting with both names)

Person	Date	Source	Comments
Jon Johanson posting as digitech	23-Sep	LividDev	Says that Drink or Die would never release code, but a friend of his has similar code and he already has a copy.
Ken Arondee	14-Jul	LinuxDVD	Shrink wrap license typically has a no RE clause?
Lodewijk Voge	20-Jul	LinuxDVD	Robocop, The Killer, Silence of the Lambs, all not CSS encrypted.
Marshall Goldberg	16-Aug	LividDev	From Sigma designs, looks to muster support for a Linux development effort with Sigma.
Martin A. Sato	24-Aug	LividDev	Agrees that segmentation of the Sigma DVD library would be good.
Martin Mueller	26-Jul	LividDev	Talks about the Pack headers and how to check for encryption.
Martin Mueller	1-Oct	LividDev	German computer magazine C'T has text about CSS (www.heise.de/ct)
Martin Mueller	2-Oct	LividDev	C't magazine says that dodsrip only contains a fraction of a player key? Www.heise.de/newsticker/data/ghi-28.09.99-000
Mathew Pavlovich	14-Jul	LinuxDVD	With full documentation for Matrox G200 cards, with the CSS disc unlocking key he can start watching DVD's.
Mathew Pavlovich	14-Jul	LinuxDVD	Merge the code with Livid
Mathew Pavlovich	15-Jul	LinuxDVD	Says that Johan's code and the code on slashdot are one and the same.
Mathew Pavlovich	11-Aug	LinuxDVD	Knew status, said 2.4 has IOCTRLS for drives in it
Michael Holtz	13-Jul	LinuxDVD	Encourages Johan to release the code
Michael Holtz	15-Jul	LinuxDVD	Thinks that only big-time pirates are a problem for the industry.
Michael Holtz	16-Jul	LinuxDVD	Has a problem with the released code getting it to work.
Michael Holtz	18-Jul	LinuxDVD	Realizes that a title key is also needed.
Michael Holtz	18-Aug	LividDev	Knows, or claims to know, how powerrip and DVDRip work, by taking video out of the display windows.
Michael Holtz	5-Sep	LividDev	Talks of patents and keys. Knows the structure of VideoCrypt.
Michael Holtz	5-Sep	LividDev	Posts results of a patent search. Several interesting nuggets appear by Intel, Cirrus, Compaq and Oak.

Person	Date	Source	Comments
Michael Holtz	5-Sep	LividDev	Followed the links in Cpmag patent to http://reality.sgi.com/memec/dvd.html.
Michael Holtz	30-Sep	LividDev	Knows someone who RE'd windows driver for the Creative DXR2 and he is trying to write a windows version, but wants to remain anonymous.
Michael Holtz	1-Oct	LividDev	Wondering how anonymous folks can work together
Michael Holtz	4-Oct	LividDev	Looking for algorithm from Derek.
Michael Holtz	8-Oct	LividDev	Totally pissed off at Jon Johanson. Says that he wants to RE it himself.
MRS	29-Oct	LividDev	Looking for someone to send him a decrypted disk key from 5-20 DVDs along with matching title keys (encrypted and decrypted), wants to try something.
Nathan Laredo	1-Oct	LividDev	Writes very assertively about the nature of CSS encryption, including that the algorithm is like RC4. Also says that the ability to read the encrypted files in WIN98 is a breach of the CSS license (How does he know?).
Nathan Laredo	1-Oct	LividDev	Adds more detail in a following post to Paul.
Nathan Laredo	8-Oct	LividDev	Don't release the source as it will get a commercial company in trouble. Post an analysis of the algorithm to sci.crypt and let the them hack it. He says a "little Birdie" tells him that a linux binary of Dodsrip will be released to Linux soon.
Nathan Laredo	8-Oct	LividDev	Writes that the CSS license agreement is available from MEI.
Nathan Laredo	8-Oct	LividDev	Says that he heard a rumor that 40 players keys may soon be available.
Nicholas Strugnell	18-Aug	LividDev	Says that rippers are perfectly legal, claims knowledge that using and developing are legal. Says in CSS the algorithm is secret.
Nicholas Strugnell	18-Aug	LividDev	Is working on getting the Matrox card to work.
Paul Volcko	15-Jun	LinuxDVD	Folks at RIT are working on this project, but general stonewalling by manufacturers on support
Paul Volcko	22-Jun	LinuxDVD	Talks about CSS. Paul has access to the DVD specs (not CSS) and is checking into the licensing legalities
Paul Volcko	5-Jul	LinuxDVD	Lots of licensing talk. Talks about Andrew Veliath's work.
Paul Volcko	13-Jul	LinuxDVD	Asks some questions about CSS, thinks the encryption is DES. Starting to mentally build the system concept.

Person	Date	Source	Comments
Paul Volcko	14-Jul	LinuxDVD	Thinks Johan Addis should send the code to someone to post. Also says go for releasing it provided that it was not accomplished with access to the specs or an NDA.
Paul Volcko	14-Jul	LinuxDVD	If one is guiding others through the learning process RE is probably okay, but no direct use.
Paul Volcko	14-Jul	LinuxDVD	Apparently Johan released the code, Paul calls him brave.
Paul Volcko	15-Jul	LinuxDVD	Something happened on slashdot? 'C' code update of the authorization code has appeared
Paul Volcko	17-Jul	LinuxDVD	See LinuxTV. Disc key blocks are longer (http://linuxtv.org).
Paul Volcko	19-Jul	LinuxDVD	Talks of the disc title structure
Paul Volcko	19-Jul	LinuxDVD	DVD .ifo files in http://linuxtv.org/dvd/fs.html
Paul Volcko	11-Aug	LinuxDVD	Asking for status of the development project
Paul Volcko	16-Aug	LividDev	Mentions that DVD drive access is now enabled thanks to work done by Andrew Veliath @ RPI.
Paul Volcko	22-Aug	LividDev	Had clearly analyzed the available rippers and knows that DVDRip does ripping before decode. He surmises how they function. Says that any Linux software based DVD player would also be broken the same way.
Paul Volcko	24-Aug	LividDev	He is part of the LSDVD project. They have access to the full DVD specifications and are writing a legal player. But no CSS specs!
Paul Volcko	1-Oct	LividDev	Recognizes the nature of RE is shady and suggests that people who want to work in that space should use anonymous remailers and encryption to protect and sign their stuff.
Paul Volcko	4-Oct	LividDev	Why don't they just make a piece of cracker code so that implementations would not need to ship with a key, thus a copy on a machine could calculate a key once it is trying to be used. This way a on-enabled version (IE no key) is shipped.
Phil Burr	27-Oct	LividDev	Posts comments on brute forcing a private player key.
Ralph Giles	14-Jul	LinuxDVD	Says post the code, elsewhere if need be to protect the Linux group.
Ralph Giles	20-Jul	LinuxDVD	Highlander and Ghost in the Shell do not have CSS encryption.

MPAA 012861

Person	Date	Source	Comments
Ralph Giles	26-Aug	LividDev	Talks about a statement by Bruce Scheier who says that "crypoanalysts and hackers don't do reverse engineering". He (Paul) further seems to imply that DCD Cipher and Firewire cipher have been broken in contests. Www.counterpane.com/crypto-gram-9812.html#contests
Ralph Metzler	11-Sep	LividDev	Is doing DVB and DVD stuff has some video playing from unencrypted VOBS. Uses a hardware card and is looking for CP to happen on that card.
Rob Lohman	26-Jul	LividDev	Creative Labs drive firmware upgrade.
Robert Horning	15-Jul	LinuxDVD	Dolby has lots of lawyers. He talks about having done DVD development
Robert Horning	20-Jul	LividDev	Good discussion of legal options.
Rolando Cedillo	14-Jul	LinuxDVD	To Johan, don't public post, but could he send a private copy?
slamg ya	8-Sep	LividDev	Says he has been watching the whole time and says to look at several sites in Germany. Http://dvdsoft.de/filez/1394cp91.pdf and http://dvdsoft.de/filez/csspaper.pdf
Ted Milker	7-Oct	LividDev	Points to DeCSS source code at: http://mmadb.no/hwlpus/ MMSystem 275 /Decss.zip
Ted Milker	7-Oct	LividDev	Writes that the source WAS there as he has a copy.
Thomas "Dent" Mirlacher	4-Oct	LividDev	Put the latest version of the .ifo file parser out as source. Big disclaimer that he had no access to specs, nor did any individuals provide him info directly.
Yuging Deng	30-Oct	LividDev	Posts code for CSS-Auth which has a whole table of player key structures.

MPAA 012862